PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4385 di Mercoledì 16 gennaio 2019

La protezione dei dati nel mondo della sanità

Più volte ho fatto presente ai lettori che tutti gli studi di mercato e l'analisi degli eventi trascorsi hanno messo in evidenza come il settore della sanità sia quello dove la protezione dei dati è poco garantita. Ecco cosa è accaduto in Portogallo.

Tutti gli studi, condotti a livello mondiale, e quindi non solo in Europa o in Italia, hanno messo in evidenza come il mondo della sanità sia quello dove il rispetto delle prescrizioni in materia di protezione dei dati personali lasci molto a desiderare.

Anche chi scrive, nella sua esperienza diretta, ha sentito più di una volta frasi del tipo "mi preoccupo più della salute del paziente che della tutela della sua privacy!".

L'esame di una pesante sanzione affibbiata dall'autorità Garante portoghese ad una struttura sanitaria è oltremodo illuminante, perché mette in evidenza le numerose lacune, che potrebbero essere presenti anche in altre strutture. L'elenco puntuale di queste strutture può costituire quindi una guida per effettuare un audit interno, da parte di un responsabile della protezione dei dati di una struttura ospedaliera, e mettere a punto eventuali misure correttive.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[SWGDPR] ?#>

La commissione nazionale per la protezione dei dati ha trovato che in un centro ospedaliero erano presenti numerose violazioni delle prescrizioni del regolamento generale europeo; la sanzione applicata è, almeno alla luce dei guai riscontrati, perfino modesta, ma probabilmente ha un valore simbolico, per mettere in guardia altre strutture sulla necessità di effettuare interventi correttivi.

Ecco l'elenco puntuale delle anomalie riscontrate dagli ispettori della commissione nazionale per la protezione dei dati.

1. Non è stato reperito alcun documento che descriva una corrispondenza tra le competenze funzionali degli utenti e i profili di accesso alle informazioni; in altre parole, nel definire il profilo di un utente, che accedeva al sistema informativo sanitario, non veniva stabilita una correlazione con le competenze specifiche.
2. Non è stato trovato alcun documento che descrivesse le regole per creare gli utenti del sistema informativo dell'ospedale, vale a dire gli autorizzati al trattamento.
3. Nove dipendenti tecnici godevano di un profilo di accesso riservato al personale medico, il che permetteva a questi autorizzati al trattamento di esaminare i protocolli terapeutici di tutti i soggetti ricoverati in ospedale.
4. Le credenziali di accesso rilasciate ai medici erano uguali per tutti, indipendentemente dalla specialità del medico. Questa situazione è considerata in piena violazione del principio di protezione per impostazione predefinita, anche chiamato principio del "need to know", previsto dall'articolo 25 del regolamento.
5. Gli utenti autorizzati sotto il profilo "medico" erano 985, ma l'esame dell'organigramma dell'ospedale indica soltanto 296 medici.
6. I profili di accesso per medici, che non operavano più all'interno della struttura sanitaria, erano ancora attivi.
7. Esistevano 18 profili di accesso non attivi e l'ultimo era stato disattivato nel novembre 2016

8. Le indagini hanno messo in evidenza che la struttura sanitaria aveva operato con sistematica negligenza, ben al corrente del fatto che stava trattando i dati in modo contrario alla legge

Assai interessante è anche esaminare il ragionamento che ha portato all'applicazione della sanzione, che tutto sommato sembra relativamente bassa, stiamo parlando di qualche centinaio di mila euro, a fronte delle violazioni riscontrate. Come i lettori sanno bene, quando si deve applicare una sanzione, occorre avviare un processo valutativo personalizzato, che prevede la bellezza di 14 parametri da esaminare.

La commissione nazionale per la produzione dei dati ha effettuato le seguenti valutazioni:

- è stato ritenuto particolarmente grave il fatto che le categorie di dati coinvolti facessero riferimento a dati particolari
- la struttura sanitaria si è attivata subito per mitigare i danni potenzialmente subiti dagli interessati coinvolti
- non vi erano precedenti violazioni riscontrate dalla commissione
- la struttura sanitaria ha cooperato in modo costruttivo con la commissione per la protezione dei dati, per mettere sotto controllo le anomalie rilevate
- le violazioni sono state riscontrate a seguito della pubblicazione di un articolo sul quotidiano locale e non a fronte di un ricorso da parte di un interessato.

È anche interessante rilevare come la commissione nazionale abbia messo in evidenza una incompatibilità giuridica, esistente in Portogallo, laddove si afferma che un'entità pubblica non può essere assoggettata a sanzioni da parte di un'altra entità pubblica. Si tratta di una situazione incredibile, che è stata messa sotto controllo da questo intervento correttivo della commissione nazionale.

Mi auguro che i lettori, coinvolti nel mondo della sanità, diano un'occhiata a questo elenco e facciano, in casa, le opportune verifiche.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.